Wave-Shaped Round Functions and Primitive Groups

Riccardo Aragona [1], Marco Calderini [2], Roberto Civino [1], Massimiliano Sala [3], and Ilaria Zappatore [4]

[1] DISIM, University of L'Aquila
[2] Department of Informatics, University of Bergen
[3] Department of Mathematics, University of Trento
[4] LIRMM of Montpellier

Abstract

Round functions used as building blocks for iterated block ciphers, both in the case of Substitution-Permutation Networks (SPN) and Feistel Networks (FN), are often obtained as the composition of different layers which provide confusion and diffusion, and key additions. The bijectivity of any encryption function, crucial in order to make the decryption possible, is guaranteed by the use of invertible layers or by the Feistel structure. In this work a new family of ciphers, called *wave ciphers*, is introduced. In wave ciphers, round functions feature *wave functions*, which are vectorial Boolean functions obtained as the composition of *non-invertible* layers, where the confusion layer enlarges the message which returns to its original size after the diffusion layer is applied. This is motivated by the fact that relaxing the requirement that all the layers are invertible allows to consider more functions which are optimal with regard to non-linearity. In particular it allows to consider injective APN S-boxes. In order to guarantee efficient decryption we propose to use wave functions in Feistel Networks. With regard to security, the immunity from some group-theoretical attacks is investigated. In particular, it is shown how to avoid that the group generated by the round functions acts imprimitively, which represents a serious flaw for the cipher. The primitivity of this group is derived as a consequence of a more general result, which allows to reduce the problem

Email adresses: ric.aragona@gmail.com (R. Aragona), marco.calderini@uib.no (M. Calderini), roberto.civino@univaq.it (R. Civino), maxsalacodes@gmail.com (M. Sala), ilaria.zappatore@lirmm.fr (I. Zappatore)

of proving that a given FN generates a primitive group to the one of proving that an SPN, directly related to the given FN, generates a primitive group. Finally, a concrete instance of real-world size wave cipher is proposed as an example, and its resistance against differential and linear cryptanalysis is also established.

Keywords: Cryptosystems; Feistel Networks; Substitution-Permutation Networks; non-invertible S-boxes; Almost Perfect Non-linearity; groups generated by round functions; primitive groups.
MSC 2010: 20B15, 20B35, 94A60.

1 Introduction

Most modern block ciphers belong to two families of symmetric cryptosystems, i.e. Substitution-Permutation Networks (SPN) and Feistel Networks (FN), and are obtained as composition of round functions. Each round function is a key-dependent permutation of the plaintext space, designed in such a way to provide both confusion and diffusion (see [32]). Confusion is provided most of the times by means of a non-linear layer which applies Boolean functions, called S-boxes, whereas a linear map, called diffusion layer, provides diffusion. In order to perform decryption, invertible layers and the Feistel structure are used in SPN and FN, respectively. In the framework of SPNs, which have been widely studied in last years, especially after the selection process for the NIST standard AES [20], decryption is performed by applying in reverse order the inverse of each layer of the cipher. In the case of FNs, it is the Feistel structure itself that guarantees a fast decryption.

Motivation and design principles It is well-known that the non-linearity of the confusion layer is a crucial parameter for the security of the cipher. In particular, in order to prevent statistical attacks (e.g. differential [8] and linear [26] cryptanalysis), block ciphers' designers are interested in invertible S-boxes reaching the best possible differential uniformity, which is two. Functions satisfying such property are called almost-perfect non-linear (APN) [27] and are extensively studied. Unfortunately, APN permutations are known only when the dimension s of the input space for the S-box is an odd number, except for the case of the Dillon's function ($s = 6$) [9], which nowadays represents the only isolated case [15]. It has been shown that no permutation with $s = 4$ is APN [13, 24] and the problem is still without answers for $s \geq 8$. On the other hand, the cases when $s \in \{4, 8\}$ are the most used for implementation reasons.
In this paper we show how to define ciphers whose S-boxes are injective APN functions with s inputs, s even. We do this by considering non-invertible S-boxes, focusing on injective confusion layers which enlarge the message. Notice that a similar approach is considered in the block cipher CAST-128, where 8×32 are used [1]. After the confusion layer is applied, a surjective diffusion layer reduces the message to its original size. By appending a key addition to the previous layers, we

obtain a vectorial Boolean function which we call a *wave function*. Consequently a *wave cipher* is a block cipher featuring wave functions in its structure. In order to guarantee an efficient decryption, we propose to use wave functions inside an FN-like framework. The opposite scenario has been considered in DES [22] and Picaro [30], where an expanding linear layer is followed by a compressing confusion layer.

Algebraic security Algebraic attacks might also represent serious threats, as we elaborate further below. It is possible to link some algebraic properties of confusion / diffusion layers and some algebraic weaknesses of the corresponding cipher. Firstly, in 1975 Coppersmith and Grossman [19] considered a set of functions which can be used to define a block cipher and, by studying the permutation group generated by those, they opened the way to a new branch of research focused on group-theoretical properties which can reveal weaknesses of the cipher itself. As it has been proved in [25], if such a group is too small, then the cipher is vulnerable to birthday-paradox attacks. Recently, in [12] the authors proved that if such group is contained in an isomorphic image of the affine group of the message space induced by a hidden sum, then it is possible to embed a dangerous trapdoor on it. More relevant in [28], Paterson built a DES-like cipher, resistant to both linear and differential cryptanalysis, whose encryption functions generate an imprimitive group and showed how the knowledge of this trapdoor can be turned into an efficient attack to the cipher. For this reason, a branch of research in Symmetric Cryptography is focused on showing that the group generated by the encryption functions of a given cipher is primitive and not of affine type (see [4, 5, 6, 11, 17, 18, 31, 33, 34, 35]). In this sense, our purpose is to give sufficient conditions for the primitivity of the group generated by the round functions of a wave cipher. These conditions result naturally from our general investigation of the link between the primitivity of the group generated by the rounds of an SPN and that of an FN. In particular, we prove a general result which links the primitivity of the group generated by the round functions of an FN and the primitivity of the group generated by the rounds of an SPN-like cipher, whose round functions are the ones performed within each round of the FN.
In this paper we aim at proving that it is possible to define a new family of block ciphers, which may feature injective APN S-Boxes of even size, whose round functions generate a primitive group. We propose a general framework for block ciphers which produces provably secure ciphers, under some cryptographic assumptions, with respect to the imprimitivity attack. In order to prove the security of the given wave cipher with respect to other classical statistical attacks (e.g. linear and differential cryptanalysis), it is needed to analyse the single instance under consideration.

Description of the paper The paper is organised as follows:

- In Section 2 our notation is presented, as well as some basic definitions and results concerning the non-linearity of Boolean functions and primitive permutations group. In particular, after having presented the main differences

between SPNs and FNs, we introduce a notion of *classical round function*, which allows to describe formally both cipher families in a unified way, provided the round key is used as a translation (i.e., the key addition is the usual XOR).

- Section 3 includes our definitions of wave functions and wave ciphers. We also show an example of an APN 4×5 S-box, which is suitable for building a strong wave function.
- In Section 4 a group-theoretical result is shown, which, as a consequence, links the primitivity of the action of an SPN with that of an FN (Theorem 4.5). Thanks to Theorem 4.5, we prove that the group generated by the round functions of a wave cipher is primitive under some standard cryptographic assumptions on the underlying wave functions (Theorem 4.9).
- In Section 5 it is designed a concrete example of 64-bit wave cipher by selecting an APN 4×5 S-box and a 40×32 diffusion layer, and its resistance against differential and linear cryptanalysis is proved.
- Section 6 concludes the paper and discusses some open problems.

2 Notation and preliminaries

Throughout this paper we use the postfix notation for every function evaluation, i.e. if f is a function and x an element in the domain of f, we denote by xf the evaluation of f in x. We denote by $\operatorname{Im} f$ the range of f and by Yf^{-1} the pre-image of a set Y.

A *block cipher* Φ is a family of key-dependent permutations

$$\{E_K \mid E_K : \mathcal{M} \to \mathcal{M},\, K \in \mathcal{K}\},$$

where $\mathcal{M}$ is the message space, $\mathcal{K}$ the key space, and $|\mathcal{M}| \leq |\mathcal{K}|$. The permutation E_K is called the *encryption function induced by the master key* K. The block cipher Φ is called an iterated block cipher if there exists $r \in \mathbb{N}$ such that for each $K \in \mathcal{K}$ the encryption function E_K is the composition of r round functions, i.e. $E_K = \varepsilon_{1,K}\, \varepsilon_{2,K} \ldots \varepsilon_{r,K}$. To provide efficiency, each round function is the composition of a public component provided by the designers, and a private component derived from the user-provided key by means of a public procedure known as *key-schedule*.

In the theory of modern iterated block cipher, two frameworks are mainly considered: Substitution-Permutation Networks (see e.g. AES [20], SERPENT [2], PRESENT [10]) and Feistel Networks (see e.g. Camelia [3], GOST [21]). Figure 1 depicts the more general framework of SPNs, FNs and their round functions; one can note that inside the round function of an FN, a function called F-function is applied to a half of the state. In both cases, the principles of confusion and diffusion

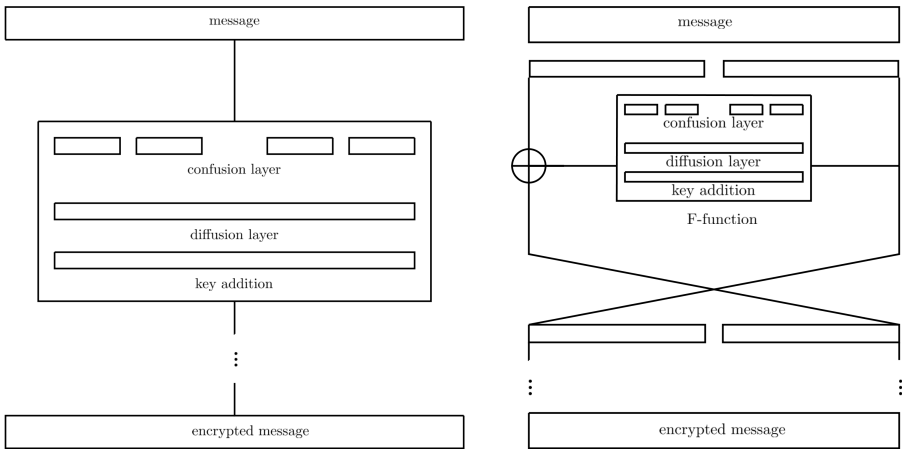

Figure 1: Round function of an SPN and of an FN

suggested by Shannon [32] are implemented by considering each round function / F-function as the composition of key-induced permutation as well as non-linear confusion layers and linear diffusion layers, which are invertible in the case of SPNs and preferably (but not necessarily) invertible in the case of FNs. We now define a class of round functions for iterated block ciphers which is large enough to include the round functions of well-established SPNs e.g. AES, PRESENT, SERPENT, and the F-function of FNs like Camelia. Notice that, for sake of simplicity, atypical rounds are not considered in this description.

Let $n \in \mathbb{N}$ and let us denote $V = (\mathbb{F}_2)^n$. Let us suppose $\dim(V) = n = bs$ and let us write $V = V_1 \oplus V_2 \oplus \ldots \oplus V_b$ where for $1 \leq j \leq b$, $\dim(V_j) = s$ and $\oplus$ represents the direct sum of vector subspaces. The subspaces V_j's are called *bricks*. We denote by $\mathrm{Sym}(V)$ the symmetric group acting on V, i.e. the group of all permutations on V. Let us also denote by $\mathrm{AGL}(V)$ the group of all affine permutations of V, which is a primitive maximal subgroup of $\mathrm{Sym}(V)$.

Definition 2.1. *For each $k \in V$, a* classical round function *induced by k is a map $\varepsilon_k \in \mathrm{Sym}(V)$ where $\varepsilon_k = \gamma\lambda\sigma_k$ and*

- *$\gamma : V \to V$ is a non-linear permutation (parallel S-box) which acts in parallel way on each V_j, i.e.*

$$(x_1, x_2, \ldots, x_n)\gamma = \big((x_1, \ldots, x_s)\gamma_1, \ldots, (x_{s(b-1)+1}, \ldots, x_n)\gamma_b\big).$$

  The maps $\gamma_j : V_j \to V_j$ are traditionally called S-boxes,

- *$\lambda \in \mathrm{Sym}(V)$ is a linear map,*

- *$\sigma_k : V \to V, x \mapsto x + k$ represents the addition with the round key k, where $+$ is the usual bitwise* XOR*.*

When used inside block ciphers, the round keys in V are derived by the designer-provided key-scheduling function from the master key $K \in \mathcal{K}$. Since, as we will discuss later in detail, studying the role of the key-schedule is out of the scopes of this paper, one can simply suppose that round keys are stochastically independent randomly-generated vectors in V.

In modern literature, terms "SPN" and "FN" may refer to a very diverse variety of ciphers. For the purposes of this paper we choose to focus only on ciphers with a XOR-based key addition. For this reason, saying SPN we refer to any cipher $\{E_K \mid K \in \mathcal{K}\} \subseteq \mathrm{Sym}(\mathcal{M})$ having an SPN-like structure with $\mathcal{M} = V$ and having classical round functions on V as round functions, and saying FN to any cipher $\{E_K \mid K \in \mathcal{K}\} \subseteq \mathrm{Sym}(\mathcal{M})$ having an FN-like structure with $\mathcal{M} = V \times V$ and having classical round functions on V as F-functions. Notice that SPNs featuring a XOR-based key addition have been also called *translation-based ciphers* in [18].

It is well-established that the security from standard statistical attacks comes from the interaction between the high non-linearity of the confusion layer and the avalanche effect guaranteed by the diffusion layer. The following section is a quick overview on one of the most used notions of non-linearity for Boolean functions, which is mainly used to prevent differential cryptanalysis [8] and other statistical attacks.

2.1 Notions of non-linearity for Boolean functions

Let $f : (\mathbb{F}_2)^s \to (\mathbb{F}_2)^t$ be a vectorial Boolean function and $u \in (\mathbb{F}_2)^s$. The derivative of f in the direction u, denoted by $\hat{f}_u$, is the function

$$\begin{array}{rccc} \hat{f}_u : & (\mathbb{F}_2)^s & \to & (\mathbb{F}_2)^t \\ & x & \mapsto & xf + (x+u)f. \end{array}$$

The following definitions can give an estimate of the non-linearity of f (see [27]).

Definition 2.2. *Let $f : (\mathbb{F}_2)^s \to (\mathbb{F}_2)^t$, $u \in (\mathbb{F}_2)^s$ and $v \in (\mathbb{F}_2)^t$. Let us define*

$$\delta_f(u,v) \stackrel{\text{def}}{=} |\{x \in (\mathbb{F}_2)^s \mid x\hat{f}_u = v\}| = |v\hat{f}_u^{-1}|.$$

The difference distribution table (DDT) *of f is the integer table*

$$\mathrm{DDT}[u,v] \stackrel{\text{def}}{=} \delta_f(u,v).$$

The differential uniformity *of f is*

$$\delta(f) \stackrel{\text{def}}{=} \max_{u \neq 0} \mathrm{DDT}[u,v],$$

and f is said δ-differentially uniform *if $\delta = \delta(f)$.*

It is well-known that $\delta(f) \geq 2$, and functions reaching the bound $\delta(f) = 2$ are called *almost perfect non-linear (APN)*. Furthermore, it is easy to show that, if f is δ-differentially uniform, then for each $u \in (\mathbb{F}_2)^s \setminus \{0\}$

$$|\operatorname{Im}(\hat{f}_u)| \geq \frac{2^s}{\delta}.$$

The requirement of Definition 2.2 is essentially a condition on the pre-images of the derivatives of f. Alternative definitions focused on the images of the derivatives of f has been given e.g. in [16, 18]. In particular, a function f satisfying

$$|\operatorname{Im}(\hat{f}_u)| > \frac{2^{s-1}}{\delta}$$

for each $u \in (\mathbb{F}_2)^s \setminus \{0\}$ is called *weakly δ-differentially uniform* [18]. It is straightforward to verify that if f is δ-differentially uniform, then it is also weakly δ-differentially uniform.

2.2 Group generated by the round functions

As already explained in Section 1, statistical attacks are just some of the issues that can threaten block ciphers. Several researchers have shown in recent years that also algebraic attacks can be effective. In this paper we focus on a particular group-theoretical attack, described in [28], based on a undesirable property of the permutation group generated by the round functions of a cipher, the *imprimitivity*.

Let $\Phi = \{E_K \mid K \in \mathcal{K}\} \subseteq \operatorname{Sym}(\mathcal{M})$ be an r-round iterated block cipher. We have stressed that the group generated by all encryption functions

$$\Gamma(\Phi) \stackrel{\text{def}}{=} \langle E_K \mid K \in \mathcal{K} \rangle \leq \operatorname{Sym}(\mathcal{M})$$

can reveal weaknesses of the cipher. However, the study of $\Gamma(\Phi)$ is not an easy task in general, since it strongly depends on the key-scheduling function (for an example of a key-schedule related study, see [7]). Hence one focuses on a group which is strictly related to $\Gamma(\Phi)$, which allows to ignore the effect of the key-schedule. For this reason, we do not discuss any key-schedule from now on. Since each permutation E_K is the composition of r round functions $\varepsilon_{1,K}, \varepsilon_{2,K} \ldots, \varepsilon_{r,K}$, for each $1 \leq h \leq r$, it is possible to define the group

$$\Gamma_h(\Phi) \stackrel{\text{def}}{=} \langle \varepsilon_{h,K} \mid K \in \mathcal{K} \rangle,$$

where all the possible round keys for round h are considered, and so the group

$$\Gamma_\infty(\Phi) \stackrel{\text{def}}{=} \langle \Gamma_h(\Phi) \mid 1 \leq h \leq r \rangle.$$

Imprimitive groups

We recall some basic notions from permutation group theory. Let G be a finite group acting on the set $\mathcal{M}$. For each $g \in G$ and $v \in \mathcal{M}$ we denote the action of g on v as vg. We denote by $vG = \{vg \mid g \in G\}$ the orbit of $v \in \mathcal{M}$ and by $G_v = \{g \in G \mid vg = v\}$ its stabiliser. The group G is said to be *transitive* on $\mathcal{M}$ if for each $v, w \in \mathcal{M}$ there exists $g \in G$ such that $vg = w$. A partition $\mathcal{B}$ of $\mathcal{M}$ is *trivial* if $\mathcal{B} = \{\mathcal{M}\}$ or $\mathcal{B} = \{\{v\} \mid v \in \mathcal{M}\}$, and *$G$-invariant* if for any $B \in \mathcal{B}$ and $g \in G$ it holds $Bg \in \mathcal{B}$. Any non-trivial and G-invariant partition $\mathcal{B}$ of $\mathcal{M}$ is called a *block system*. In particular any $B \in \mathcal{B}$ is called an *imprimitivity block*. The group G is *primitive* in its action on $\mathcal{M}$ (or G *acts primitively* on $\mathcal{M}$) if G is transitive and there exists no block system. Otherwise, the group G is *imprimitive* in its action on $\mathcal{M}$ (or G *acts imprimitively* on $\mathcal{M}$). We recall the following well-known results which will be useful in the remainder of the paper, and whose proofs may be found e.g. in [14].

Lemma 2.3. *A block of imprimitivity is the orbit vH of a proper subgroup $H < G$ that properly contains the stabiliser G_v, for some $v \in \mathcal{M}$.*

Lemma 2.4. *If T is a transitive subgroup of G, then a block system for G is also a block system for T.*

Lemma 2.5. *Let us assume that $\mathcal{M}$ is a finite vector space over $\mathbb{F}_2$ and T its translation group, i.e. $T = \{\sigma_v \mid \sigma_v : \mathcal{M} \to \mathcal{M},\ x \mapsto x + v, v \in \mathcal{M}\}$. The group T is transitive and imprimitive on $\mathcal{M}$. Moreover, for any proper and non-trivial subgroup U of $(\mathcal{M}, +)$, $\{U + v \mid v \in \mathcal{M}\}$ is a block system.*

Imprimivity attack

The cryptanalysts' interest into the imprimitivity of the group generated by the round functions of a block cipher arise from the study performed in [28], where it is showed how the imprimitivity of the group can be exploited to construct a trapdoor that may be hard to detect. In particular, the author gave an example of a DES-like cipher, which can be easily broken since its round functions generate an imprimitive group, but which is resistant to both linear and differential cryptanalysis.

3 Wave ciphers

The aim of this section is to define ciphers whose inner layers are not necessarily invertible, in order to use APN vectorial Boolean functions as S-boxes (even when the S-box input size is four or eight). We focus on the case of wave-shaped round functions, which feature a first layer which enlarges the state, a second which reduces its size, and a key addition. These round functions are employed in the place of classical round functions for both SPNs and FNs. To do so, let us recall that $n = bs \in \mathbb{N}$ and $V = (\mathbb{F}_2)^n$, where $V = V_1 \oplus V_2 \oplus \ldots \oplus V_b$, for $1 \leq j \leq b$, and $\dim(V_j) = s$. Let us define an auxiliary space $W = (\mathbb{F}_2)^m$, with $n \leq m$ such that $\dim(W) = m = bt$ and $W = W_1 \oplus W_2 \oplus \ldots \oplus W_b$. The subspaces W_j's, as the subspaces V_j's, are called

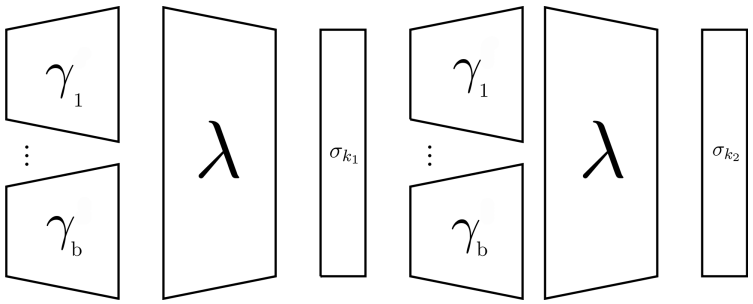

Figure 2: Wave functions

bricks.

What follows is a generalisation of the concept of classical round function.

Definition 3.1. *For each $k \in V$, the* wave function *induced by k is a map $\varepsilon_k : V \to V$, where $\varepsilon_k = \gamma\lambda\sigma_k$ and*

- *$\gamma : V \to W$ is an injective non-linear transformation (parallel S-box) which acts in parallel way on each V_j, i.e.*

$$(x_1, x_2, \ldots, x_n)\gamma = \big((x_1, \ldots, x_s)\gamma_1, \ldots, (x_{s(b-1)+1}, \ldots, x_n)\gamma_b\big).$$

  The maps $\gamma_j : V_j \to W_j$ are called S-boxes;

- *$\lambda : W \to V$ is a surjective linear map;*

- *$\sigma_k : V \to V, x \mapsto x + k$ is the round key addition.*

Figure 2 depicts the composition of two consecutive wave functions.

Notice that, although the hypothesis of each layer being singularly invertible may be relaxed, decryption is granted only if each wave function is overall invertible. The following result gives a condition on the confusion and diffusion layers which ensures that a wave function is a permutation.

Lemma 3.2. *Let $\varepsilon_k = \gamma\lambda\sigma_k$ be a wave function. The following are equivalent:*

1. *$\{a + b \mid a, b \in \operatorname{Im}\gamma\} \cap \operatorname{Ker}\lambda = \{0\}$;*
2. *$\varepsilon_k \in \operatorname{Sym}(V)$.*

Proof. Let us assume 1. Let $x_1, x_2 \in V$ such that $x_1\varepsilon_k = x_2\varepsilon_k$. Then $(x_1\gamma + x_2\gamma)\lambda = 0$, so $x_1\gamma + x_2\gamma \in \{a + b \mid a, b \in \operatorname{Im}\gamma\} \cap \operatorname{Ker}\lambda = \{0\}$, and hence $x_1\gamma = x_2\gamma$. Since γ is injective, it follows $x_1 = x_2$. Conversely, let $x \in \{a + b \mid a, b \in \operatorname{Im}\gamma\} \cap \operatorname{Ker}\lambda$. Then there exist $x_1, x_2 \in V$ such that $x = x_1\gamma + x_2\gamma$ and $x\lambda = 0$, that is $x_1\gamma\lambda = x_2\gamma\lambda$. Therefore $x_1\varepsilon_k = x_2\varepsilon_k$ and hence $x_1 = x_2$, which implies $x = 0$. □

x	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
$x\gamma_1$	0_x	B_x	$1B_x$	8_x	$1D_x$	17_x	12_x	4_x	D_x	14_x	1_x	$1E_x$	18_x	2_x	E_x	7_x

Figure 3: A 4x5 APN S-box

Remark 3.3. Notice that it always holds $0 \in \{a+b \mid a,b \in \operatorname{Im}\gamma\} \cap \operatorname{Ker}\lambda$. Moreover, notice that if we assume that $0\gamma = 0$, then the first condition of the previous lemma implies that $\operatorname{Im}\gamma \cap \operatorname{Ker}\lambda = \{0\}$.

3.1 Using a 4x5 APN function

The function $\gamma_1 : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^5$ displayed in Figure 3 represents an example of a 4x5 injective function, which is APN, as it can be noted looking at its DDT displayed in Table 1 in the last page of this paper. Each vector is interpreted as a binary number, most significant bit first, and then represented using the hexadecimal notation (e.g. $(0,0,0,1) = 1_x$). With an eye on using this function as an S-box for a wave function, one has to verify that there exists a diffusion layer satisfying the hypothesis of Lemma 3.2. It holds $\operatorname{Im}(\gamma_1) \subset (\mathbb{F}_2)^5$; moreover it is easy to check that $|\{a+b \mid a,b \in \operatorname{Im}(\gamma_1)\}| = 31$, and the missing vector in $(\mathbb{F}_2)^5$ is $\xi \stackrel{\text{def}}{=} 11_x$. A possible way to design a cipher whose confusion layer applies in parallel b copies of the S-box γ_1 is to determine a diffusion layer λ whose null space is $\operatorname{Span}_{\mathbb{F}_2}\{(\xi,0,\ldots,0),(0,\xi,0,\ldots,0),\ldots,(0,0,\ldots,\xi)\}$, where 0 denotes the zero vector in $(\mathbb{F}_2)^5$. The hypothesis 1 of Lemma 3.2 is satisfied, hence all the produced wave functions are bijective. Such a diffusion layer features a *parallel* kernel, i.e.

$$\operatorname{Ker}\lambda = \bigoplus_{j=1}^{b} \operatorname{Ker}\lambda \cap W_j.$$

This important feature will be also exploited in the following sections.
Notice that it is not hard to find examples of such APN functions. Indeed, it is possible to construct an APN map $\gamma : (\mathbb{F}_2)^n \to (\mathbb{F}_2)^{n+1}$ by considering first a function defined over $(\mathbb{F}_2)^n$ and then extending its image to $(\mathbb{F}_2)^{n+1}$ by adding an extra bit. Otherwise it is possible to embed $(\mathbb{F}_2)^n$ into $(\mathbb{F}_2)^{n+1}$ and then consider an APN map defined over $(\mathbb{F}_2)^{n+1}$. The map γ_1 has been obtained using the first approach on the power function $x \mapsto x^{-1}$.

3.2 Feistel Networks with wave functions

Since our goal is to use the previously defined wave functions inside a cipher, we now define a *wave cipher* as an FN whose F-function is a wave function. Feistel Network's straightforward decryption encourages this choice.

Before defining wave ciphers, we generalise a standard security requirement for diffusion layers [18] to the case of surjective maps.

Definition 3.4. *A* wall *of V (resp. W) is any non-trivial and proper sum of bricks of V (resp. W). A surjective linear transformation $\lambda : W \longrightarrow V$ is a* proper diffusion layer *if for any wall $W' = \bigoplus_{j\in I} W_j$ of W and $V' = \bigoplus_{j\in I} V_j$ of V, where $I \subset \{1, \ldots, b\}$, then*

$$V'\lambda^{-1} \nsubseteq W' + \operatorname{Ker}\lambda.$$

In other terms, if $\pi : W \longrightarrow W/\operatorname{Ker}\lambda$ is the *canonical projection of* W onto $W/\mathrm{Ker}(\lambda)$, λ is proper if there exists no wall $W' = \bigoplus_{j\in I} W_j$ of W and $V' = \bigoplus_{j\in I} V_j$ of V such that $W'\pi\lambda = V'$.

We are now ready to define our new class of block ciphers, having $\mathcal{M} = V \times V$ as message space. In what follows, 0_n and 1_n denote the zero matrix of size $n \times n$ and the identity matrix of size n respectively. Moreover, for any given function $f : (\mathbb{F}_2)^n \to (\mathbb{F}_2)^n$, we denote by $\overline{f}$ the formal operator $\overline{f} : (\mathbb{F}_2)^{2n} \to (\mathbb{F}_2)^{2n}$

$$\overline{f} \stackrel{\text{def}}{=} \begin{pmatrix} 0_n & 1_n \\ 1_n & f \end{pmatrix},$$

such that for any $(x_1, x_2) \in (\mathbb{F}_2)^n \times (\mathbb{F}_2)^n$ acts as $(x_1, x_2)\overline{f} = (x_2, x_1 + x_2 f)$. The latter is called the *Feistel operator induced by* f and, as we will discuss further, allows to give an algebraic description of FNs.

Definition 3.5. *An r-round wave cipher Φ is a family of encryption functions $\{E_K \mid K \in \mathcal{K}\} \subseteq \mathrm{Sym}(V \times V)$ such that for each $K \in \mathcal{K}$ the map E_K is the composition of r functions. More precisely $E_K = \overline{\varepsilon_{1,K}}\,\overline{\varepsilon_{2,K}} \ldots \overline{\varepsilon_{r,K}}$, where $\varepsilon_{i,K} = \gamma\lambda\sigma_{k_i}$ is an n-bit wave function such that*

- *λ is a proper diffusion layer,*
- *the key-schedule $\mathcal{K} \to V^r$, $K \mapsto (k_1, k_2, \ldots, k_r)$, is surjective w.r.t. any round.*

The function $\rho \stackrel{\text{def}}{=} \gamma\lambda$ is called the generating function *of the cipher.*

Let us notice that the ciphers previously introduced are FNs featuring a wave function as F-function. Indeed, given $(x_1, x_2) \in V \times V$ one has

$$(x_1, x_2)\overline{\varepsilon_{i,K}} = (x_1, x_2)\begin{pmatrix} 0_n & 1_n \\ 1_n & \varepsilon_{i,K} \end{pmatrix} = (x_2, x_1 + x_2\varepsilon_{i,K}),$$

where the operator $\overline{\varepsilon_{i,K}}$ induces the Feistel structure, as shown in Figure 4. Moreover $\overline{\varepsilon_{i,K}}$ is invertible with the following inverse

$$\overline{\varepsilon_{i,K}}^{-1} = \begin{pmatrix} \varepsilon_{i,K} & 1_n \\ 1_n & 0_n \end{pmatrix}.$$

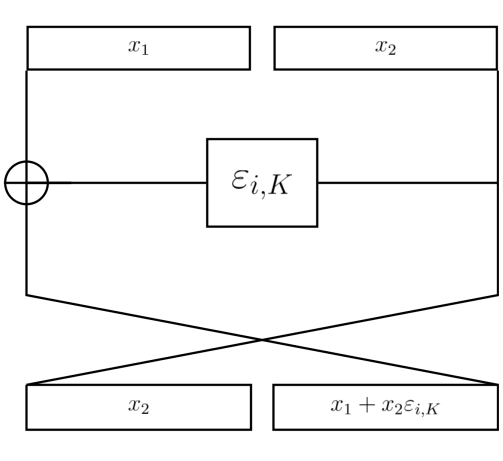

Figure 4: Feistel structure of wave ciphers

It is indeed an easy check that

$$(x_2, x_1 + x_2\varepsilon_{i,K}) \begin{pmatrix} \varepsilon_{i,K} & 1_n \\ 1_n & 0_n \end{pmatrix} = (x_1, x_2).$$

Note that, as for any FN, the inverse $\overline{\varepsilon_{i,K}}^{-1}$ of the round function $\overline{\varepsilon_{i,K}}$ does not involve the inverse of the wave function $\varepsilon_{i,K}$.

Remark 3.6. Let $T_{(0,n)} \stackrel{\text{def}}{=} \{\sigma_{(0,k)} \mid (x_1, x_2) \mapsto (x_1, x_2 + k)\} < \mathrm{Sym}(V \times V)$. Let ρ be the generating function of a wave cipher Φ, and $\overline{\rho}$ the corresponding Feistel operator

$$\overline{\rho} = \begin{pmatrix} 0_n & 1_n \\ 1_n & \rho \end{pmatrix}.$$

Then $\overline{\varepsilon_{i,K}} = \overline{\rho}\,\sigma_{(0,k_i)}$, and so $\langle T_{(0,n)}, \overline{\rho} \rangle$ is the group generated by the round functions of the wave cipher Φ.

4 Group-theoretical study of Wave ciphers

In this section, first we show a group-theoretical result which, as consequence, links the primitivity for a Substitution-Permutation Network and the primitivity for a Feistel Network having respectively round functions and F-functions with the same structure. By exploiting this result we prove that the group generated by the round functions of a wave cipher is primitive under some reasonable cryptographic assumptions on the underlying wave functions.

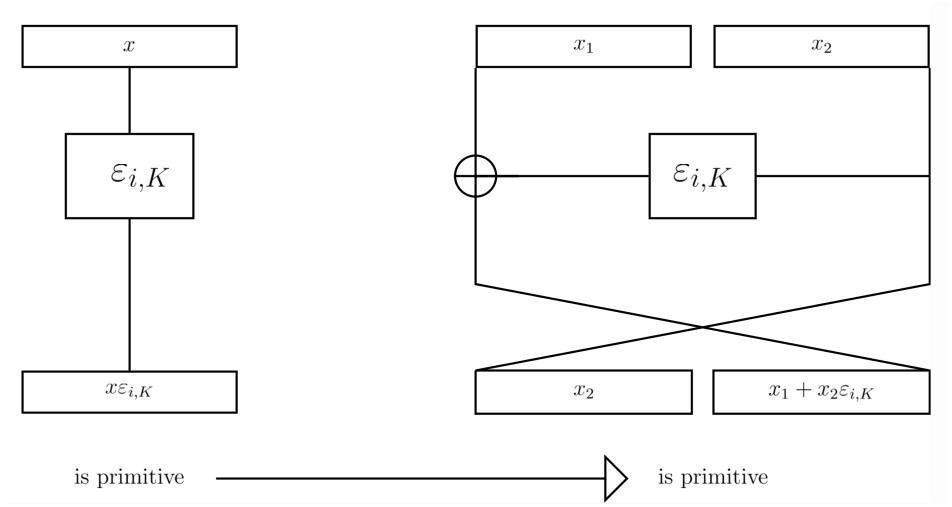

Figure 5: Feistel to SPN reduction

4.1 Security reduction

Let us consider the group generated by the rounds of an FN which uses as F-functions the round functions of a primitive SPN. Here we prove a group-theoretical result which implies the primitivity of this group under the assumption that the wave functions are invertible. In particular this result is used to show that the group generated by the round functions of a wave cipher is primitive if the group[1] generated by the round functions of an SPN-like cipher having as round functions the same wave functions is primitive, as depicted in Fig. 5.

Let us recall that $T_{(0,n)} = \{\sigma_{(0,k)} \mid (x_1, x_2) \mapsto (x_1, x_2 + k)\} < \mathrm{Sym}(V \times V)$ and define

- $T_n \stackrel{\text{def}}{=} \{\sigma_k \mid x \mapsto x + k\} < \mathrm{Sym}(V)$,
- $T_{(n,0)} \stackrel{\text{def}}{=} \{\sigma_{(k,0)} \mid (x_1, x_2) \mapsto (x_1 + k, x_2)\} < \mathrm{Sym}(V \times V)$,
- $T_{(n,n)} \stackrel{\text{def}}{=} \{\sigma_{(k_1,k_2)} \mid (x_1, x_2) \mapsto (x_1 + k_1, x_2 + k_2)\} < \mathrm{Sym}(V \times V)$.

Notice that $T_n \cong T_{(0,n)} \cong T_{(n,0)} < T_{(n,n)}$.

Let ρ be any element in $\mathrm{Sym}(V)$, $\overline{\rho}$ be the corresponding Feistel operator, and let $\Gamma \stackrel{\text{def}}{=} \langle T_{(0,n)}, \overline{\rho} \rangle$. Since we aim at characterising imprimitivity blocks for Γ using

[1] Note that the hypothesis that the wave functions are invertible allows to consider this group.

Lemma 2.4 and Lemma 2.5, we need to individuate a transitive subgroup of Γ. For this reason, the following alternative presentation of Γ is useful.

Lemma 4.1. $\Gamma = \langle T_{(n,n)}, \overline{\rho} \rangle$.

Proof. Obviously $\Gamma = \langle T_{(0,n)}, \overline{\rho} \rangle < \langle T_{(n,n)}, \overline{\rho} \rangle$. On the other hand, given $x_1, x_2, k \in V$ one has

$$\begin{aligned}(x_1, x_2)\overline{\rho}\sigma_{(0,k)} =& (x_1, x_2)\begin{pmatrix} 0_n & 1_n \\ 1_n & \rho \end{pmatrix}\sigma_{(0,k)} \\ =& (x_2, x_1 + x_2\rho + k) \\ =& (x_1 + k, x_2)\begin{pmatrix} 0_n & 1_n \\ 1_n & \rho \end{pmatrix} \\ =& (x_1, x_2)\sigma_{(k,0)}\overline{\rho}.\end{aligned}$$

Hence for each $k \in V$ it holds $\overline{\rho}\sigma_{(0,k)} = \sigma_{(k,0)}\overline{\rho}$, and consequently $\sigma_{(k,0)} \in \Gamma$. Therefore for each $k_1, k_2 \in V$, $\sigma_{(k_1,k_2)} = \sigma_{(k_1,0)}\sigma_{(0,k_2)} \in \Gamma$. □

Being $T_{(n,n)}$ a transitive subgroup of Γ and noticing that the subgroups of $T_{(n,n)}$ are of the form $\{\sigma_u : u \in U\}$, where U is a subgroup of $V \times V$, we obtain the following.

Lemma 4.2. *If Γ is imprimivitive in its action on $V \times V$, then a block system is made of the cosets of a subgroup of $V \times V$, i.e. it is*

$$\{U + v \mid v \in V \times V\},$$

where U is a non-trivial and proper subgroup of $V \times V$.

Proof. See Lemma 2.4 and Lemma 2.5. □

According to Lemma 4.2, in order to prove that Γ is primitive it is sufficient to prove that no subgroup of $V \times V$ is a block. The following theorem, due to Goursat [23, Sections 11–12], characterises the subgroups of the direct product of two groups in terms of suitable sections of the direct factors (see also [29]). We apply this result to the additive group $V \times V$.

Theorem 4.3 (Goursat's Lemma [23])**.** *Let G_1 and G_2 be two groups. There exists a bijection between*

1. *the set of all subgroups of the direct product $G_1 \times G_2$, and*
2. *the set of all triples $(A/B, C/D, \psi)$, where*
   - *A is a subgroup of G_1,*
   - *C is a subgroup of G_2,*
   - *B is a normal subgroup of A,*
   - *D is a normal subgroup of C, and*

- $\psi : A/B \to C/D$ *is a group isomorphism.*

In this bijection, each subgroup of $G_1 \times G_2$ *can be uniquely written as*

$$U_\psi = \{(a, c) \in A \times C : (a + B)\psi = c + D\}.$$

Note that the isomorphism $\psi : A/B \to C/D$ is induced by a homomorphism $\varphi : A \to C$ such that $(a + B)\psi = a\varphi + D$ for any $a \in A$, and $B\varphi \leq D$. Such homomorphism is not unique.

Lemma 4.4. *In the above notation, given any homomorphism* φ *inducing* ψ*, we have*

$$U_\psi = \{(a, a\varphi + d) : a \in A, d \in D\}. \tag{1}$$

Proof. Note first that the right-hand side of (1) is contained in U_ψ, since for $a \in A$ and $d \in D$ we have $(a + B)\psi = a\varphi + D = a\varphi + d + D$, that is, $(a, a\varphi + d) \in U_\psi$. Moreover U_ψ is contained in the right-hand side of (1). Indeed, if $(a, c) \in U_\psi$ we have $a\varphi + D = (a + B)\psi = c + D$, so that $c = a\varphi + d$ for some $d \in D$. □

This is our main result of this section.

Theorem 4.5. *Let* $\rho \in \mathrm{Sym}(V) \setminus \mathrm{AGL}(V)$*,* $\overline{\rho}$ *be the corresponding Feistel operator, and denote by* $\Gamma = \langle T_n, \rho \rangle$ *and by* $\overline{\Gamma} = \left\langle T_{(0,n)}, \overline{\rho} \right\rangle$*. If* Γ *is primitive on* V*, then* $\overline{\Gamma}$ *is primitive on* $V \times V$*.*

Before proving Theorem 4.5, we show how this group-theoretical result can be helpful to us. Let $\Phi = \{E_K \mid K \in \mathcal{K}\} \subseteq \mathrm{Sym}(V \times V)$ be an r-round wave block cipher with a bijective generating function $\rho = \gamma\lambda$. By Remark 3.6 one has that $\Gamma_\infty(\Phi) = \langle T_{(0,n)}, \overline{\rho} \rangle$ is the group generated by the round functions of the wave cipher Φ. Moreover, $\langle T_n, \rho \rangle$ is the group generated by the wave-shaped round functions of an SPN-like cipher whose round functions are $\varepsilon_{i,K} = \rho\sigma_{(0,k_i)}$. Therefore, from Theorem 4.5, next result directly follows.

Corollary 4.6. *Let* Φ *be a wave cipher,* $\rho \in \mathrm{Sym}(V)$ *its generating function and* $\overline{\rho}$ *the Feistel operator induced by* ρ*. If* $\langle T_n, \rho \rangle$ *is primitive on* V*, then* $\Gamma_\infty(\Phi) = \langle T_{(0,n)}, \overline{\rho} \rangle$ *is primitive on* $V \times V$*.*

Proof of Theorem 4.5. Let us suppose that $\overline{\Gamma} = \left\langle T_{(0,n)}, \overline{\rho} \right\rangle = \left\langle T_{(n,n)}, \overline{\rho} \right\rangle$ is imprimitive, so there exists a non-trivial and proper subgroup U of $V \times V = (\mathbb{F}_2)^n \times (\mathbb{F}_2)^n$ such that $\{U + (v_1, v_2) \mid (v_1, v_2) \in V \times V\}$ is a block system. In particular,

$$U\overline{\rho} = U + (v_1, v_2) \tag{2}$$

for some $(v_1, v_2) \in V \times V$. Since $(0, 0)\overline{\rho} = (0, 0\rho)$, we can assume $v_1 = 0$ and $v_2 = 0\rho$. With reference to Lemma 4.4 and its notation, we have $U = \{(a, a\varphi + d) \mid a \in A, d \in D\}$, and by (2), for any $a \in A$ and $d \in D$ there exist $x \in A$ and $y \in D$ such that

$$(a, a\varphi + d) \begin{pmatrix} 0_n & 1_n \\ 1_n & \rho \end{pmatrix} = (x, x\varphi + y + 0\rho),$$

that is

$$(a\varphi + d, a + (a\varphi + d)\rho) = (x, x\varphi + y + 0\rho).$$

Hence, it holds $x = a\varphi + d$, and considering $a = 0$, we obtain $D \leq A$. Otherwise, considering $d = 0$, we obtain $A\varphi \leq A$. Similarly, we have

$$U\overline{\rho}^{-1} = U + (v_1', v_2') \tag{3}$$

for some $(v_1', v_2') \in V \times V$. Since $\overline{\rho}^{-1} = \begin{pmatrix} \rho & 1_n \\ 1_n & 0_n \end{pmatrix}$, we can consider $v_1' = 0\rho$ and $v_2' = 0$. In this case, for any $a \in A$ and $d \in D$ there exist $x \in A$ and $y \in D$ such that

$$(a\rho + a\varphi + d, a) = (x + 0\rho, x\varphi + y).$$

Hence we have $x = a\rho + a\varphi + d + 0\rho$. Substituting $x = a\varphi + d$ in $x\varphi + y$ and being φ a homomorphism, it holds $y = a + a\rho\varphi + a\varphi^2 + d\varphi + 0\rho\varphi$. Then, considering $a = 0$, we obtain $y = d\varphi$, and thus $D\varphi \leq D$. Now, in the general case, letting $(v_1, v_2) \in V \times V$ it holds

$$(U + (v_1, v_2))\overline{\rho} = U + (v_1', v_2') \tag{4}$$

for some $(v_1', v_2') \in V \times V$. By definition of $\overline{\rho}$, we can take $v_1' = v_2$ and $v_2' = v_1 + v_2\rho$. By Lemma 4.4 and by (4), for any $a \in A$ and $d \in D$ there exist $x \in A$ and $y \in D$ such that

$$(a + v_1, a\varphi + d + v_2)\begin{pmatrix} 0_n & 1_n \\ 1_n & \rho \end{pmatrix} = (x + v_2, x\varphi + y + v_1 + v_2\rho),$$

that is,

$$(a\varphi + d + v_2, a + v_1 + (a\varphi + d + v_2)\rho) = (x + v_2, x\varphi + y + v_1 + v_2\rho),$$

hence we have $x = a\varphi + d$. Substituting $x = a\varphi + d$ in $x\varphi + y + v_1 + v_2\rho$,

$$a + v_1 + (a\varphi + d + v_2)\rho + a\varphi^2 + v_1 + v_2\rho = y + d\varphi.$$

Then, considering $a = 0$, we obtain $(d + v_2)\rho = y + d\varphi + v_2\rho$. Since $D\varphi \leq D$, then $y + d\varphi \in D$ and so

$$(D + v_2)\rho = D + v_2\rho.$$

Note that we obtain the equality since ρ is a permutation. If $D \neq \{0\}, (\mathbb{F}_2)^n$, then we proved that the imprimitivity of $\overline{\Gamma}$ implies the imprimitivity of Γ. To complete the proof, it remains to consider the cases $D = (\mathbb{F}_2)^n$ and $D = \{0\}$.

[$\mathbf{D = (\mathbb{F}_2)^n}$] We proved that $D \leq A$, and from the hypotheses holds that $D \leq C$ and ψ is an isomorphism between A/B and C/D. Since $D = (\mathbb{F}_2)^n$, we have $D = C = A = B = (\mathbb{F}_2)^n$, which contradicts that U is a proper subgroup of $V \times V$.

[$\mathbf{D = \{0\}}$] First, note that in this case $B\varphi = \{0\}$. Moreover, by Lemma 4.4,

$$U = \{(a, a\varphi) \mid a \in A\},$$

and by (4) for any $a \in A$ there exists $x \in A$ such that

$$(a\varphi + v_2, a + v_1 + (a\varphi + v_2)\rho) = (x + v_2, x\varphi + v_1 + v_2\rho).$$

Proceedings as before, it holds

$$a + a\varphi^2 = (a\varphi + v_2)\rho + v_2\rho. \tag{5}$$

Note that for any $a \in B \leq A$, $a\varphi = 0$ and so we obtain $a + v_2\rho = v_2\rho$ for any $a \in B$, that is, $B = \{0\}$. Therefore, if $D = \{0\}$, also $B = \{0\}$ and so $\varphi = \psi$ is an isomorphism between A and C. Moreover, since $A\varphi$ is contained in both A and C, then $A = C$ and φ is an automorphism of A. If $A = \{0\}$, then $A = C = D = B = \{0\}$, which contradicts that U is non-trivial. If A is a proper subgroup of $(\mathbb{F}_2)^n$, then by (5) and since both $a + a\varphi^2$ and $a\varphi$ belong to A we have

$$(A + v_2)\rho = A + v_2\rho,$$

and so Γ is imprimitive. If $A = (\mathbb{F}_2)^n$, in equation (5) we can consider $v_2 = 0$ since $a\varphi + v_2$ is an element of $A = (\mathbb{F}_2)^n$, so we have

$$(a\varphi)\rho = a + a\varphi^2 + 0\rho.$$

Since the function $x + x\varphi^2$ is linear, we proved that $\rho \in \mathrm{AGL}(V)$, which is a contradiction. □

4.2 Conditions on SPN-like wave ciphers

In the light of Theorem 4.5, given a wave cipher Φ whose generating function ρ is invertible, we obtain that the group $\Gamma_\infty(\Phi)$ is primitive if we manage to prove that the group $\langle T_n, \rho \rangle$ is primitive. The latter represents the group generated by the rounds of an SPN-like cipher featuring wave functions in the place of classical round functions. Although for such a cipher it may be difficult to compute the computational inverse of the encryption functions, since it has an SPN structure with non-invertible layers, we can still study its theoretical properties. In this section we underline which properties of the generating function ρ guarantee that $\langle T_n, \rho \rangle$ is primitive. From now on let us assume that $\rho \in \mathrm{Sym}(V)$.

Let $\rho = \gamma\lambda$ be the generating function of a wave cipher. We can always assume that γ maps 0 into 0, since it is possible to add 0γ to the round key of the previous round. Then, since λ is linear, it holds $0\rho = 0$.

In the following, we define a generalisation of the notion of strong anti-invariance given in [18], which is a condition in our second main theorem. Let us recall that, as in Section 3, $V = V_1 \oplus V_2 \oplus \ldots \oplus V_b$ and $W = W_1 \oplus W_2 \oplus \ldots \oplus W_b$, with $V_j = (\mathbb{F}_2)^s$ and $W_j = (\mathbb{F}_2)^t$ for each $j \in \{1, 2, \ldots, b\}$.

Definition 4.7. *Let $j \in \{1, 2, \ldots, b\}$, $\gamma_j : V_j \to W_j$ be an S-box such that $0\gamma_j = 0$, and $\lambda : W \to V$ be a surjective linear map. Given $0 \leq \delta < s$, γ_j is* δ-non-invariant with respect to λ *if for any proper subspaces $V' < V_j$ and $W' < W_j$ such that $V'\gamma_j + \mathrm{Ker}\,\lambda \cap W_j = W'$, then $\dim(W') < s - \delta$.*

Notice that if $0 \leq \delta < \delta' < s$ and γ_j is δ'-non-invariant w.r.t. λ, then it is also δ-non-invariant w.r.t. λ.

Lemma 4.8. *Let $\rho = \gamma\lambda \in \mathrm{Sym}(V)$ be the generating function of a wave cipher. Then $\langle T_n, \rho \rangle$ is imprimitive if and only if there exists a proper and non-trivial subgroup U of V such that $(u+v)\gamma + v\gamma \in U\lambda^{-1}$, for any $u \in U$ and $v \in V$. In this case, $\{U + v \mid v \in V\}$ is a block system for $\langle T_n, \rho \rangle$.*

Proof. Since $T_n \leq \langle T_n, \rho \rangle$, if $\langle T_n, \rho \rangle$ is imprimitive, then $\{U + v \mid v \in V\}$ is a block system, for some proper and non-trivial subgroup U of V. Let $v \in V$, then $(U+v)\rho = U + v\rho = U + v\gamma\lambda$. Therefore for any $u \in U$ and $v \in V$ it holds $(u+v)\gamma\lambda + v\gamma\lambda \in U$ and, since λ is linear, $(u+v)\gamma + v\gamma \in U\lambda^{-1}$. □

The following is the main result of this section.

Theorem 4.9. *Let $\rho = \gamma\lambda \in \mathrm{Sym}(V)$ be the generating function of a wave cipher Φ. If there exists $1 \leq \delta < s$ such that for each $j \in \{1, 2, \ldots, b\}$ the S-box γ_j is*

- *2^δ-differentially uniform,*
- *δ-non-invariant with respect to λ,*

and if $\mathrm{Ker}\,\lambda = \bigoplus_{j=1}^{b} \mathrm{Ker}\,\lambda \cap W_j$, then $\langle T_n, \rho \rangle$ is primitive (and so it is $\Gamma_\infty(\Phi)$).

Proof. Suppose that $\langle T_n, \rho \rangle$ is imprimitive. For the Lemma 4.8, a block system is of the form $\{U + v \mid v \in V\}$, for any proper non-trivial subgroup U of V. Since U is an imprimitivity block and $\rho \in \langle T_n, \rho \rangle$, $U\rho = U + v$ for some $v \in V$. Moreover, since $0\rho = 0$, we obtain $U + v = U$, and consequently $U\rho = U\gamma\lambda = U$. Moreover

$$U\gamma + \mathrm{Ker}\,\lambda = U\lambda^{-1} \subseteq W, \tag{6}$$

and so $U\gamma + \mathrm{Ker}\,\lambda$ is a subspace of W. For $1 \leq j \leq b$, let $\pi_j : V \longrightarrow V_j$ be the j-th projection with respect to the decomposition $V = V_1 \oplus \ldots \oplus V_b$, and $I \stackrel{\text{def}}{=} \{\, j \mid j \in \{1, \ldots, b\}, U\pi_j \neq \{0\}\}$. Then two cases are possible: either $U \cap V_j = V_j$ for each $j \in I$, or there exists $j \in I$ such that $U \cap V_j \neq V_j$.

In the first case $U = \bigoplus_{j \in I} V_j$ is a wall. From (6) it holds

$$(\bigoplus_{j \in I} V_j)\gamma + \mathrm{Ker}\,\lambda = (\bigoplus_{j \in I} V_j)\lambda^{-1}. \tag{7}$$

Since γ is a parallel transformation, we have

$$(\bigoplus_{j \in I} V_j)\gamma \subset \bigoplus_{j \in I} W_j. \tag{8}$$

Thus, from (7) and (8) it follows that

$$(\bigoplus_{j \in I} V_j)\lambda^{-1} \subset \bigoplus_{j \in I} W_j + \mathrm{Ker}\,\lambda,$$

which is a contradiction since λ is proper.

In the second case, let us assume there exists $j \in I$ such that $U \cap V_j \neq V_j$. From (6) we have

$$(U\gamma + \operatorname{Ker}\lambda) \cap W_j = U\lambda^{-1} \cap W_j, \tag{9}$$

where, since both γ and the kernel of λ are parallel,

$$(U\gamma + \operatorname{Ker}\lambda) \cap W_j = U\gamma \cap W_j + \operatorname{Ker}\lambda \cap W_j = (U \cap V_j)\gamma_j + \operatorname{Ker}\lambda \cap W_j. \tag{10}$$

Indeed, let $u = (u_1\gamma_1, u_2\gamma_2, \ldots, u_b\gamma_b) \in U\gamma$, $v = (v_1, v_2, \ldots, v_b) \in \operatorname{Ker}\lambda$, and let us assume that $w \stackrel{\text{def}}{=} u\gamma + v \in (U\gamma + \operatorname{Ker}\lambda) \cap W_j$, hence $w = (0, \ldots, 0, w_j, 0, \ldots, 0)$. For $l \neq j$ we obtain $u_l\gamma_l = v_l$, hence $v_l \in \operatorname{Im}\gamma_l \cap (\operatorname{Ker}\lambda \cap W_l)$. From Remark 3.3 and since $\operatorname{Ker}\lambda$ is parallel, we have $\operatorname{Im}\gamma_l \cap (\operatorname{Ker}\lambda \cap W_l) = \{0\}$, therefore $v_l = u_l = 0$. Thus, (9) and (10) imply that

$$(U \cap V_j)\gamma_j + \operatorname{Ker}\lambda \cap W_j = U\lambda^{-1} \cap W_j,$$

and, since γ_j is δ-non-invariant with respect to λ, then

$$\dim(U\lambda^{-1} \cap W_j) < s - \delta. \tag{11}$$

Furthermore, let $u \in U$ such that $u_j \stackrel{\text{def}}{=} u\pi_j \neq 0$ and $v_j \in V_j$. Since $\langle T_n, \rho \rangle$ is imprimitive, by Lemma 4.8 it follows that $(u + v_j)\gamma + v_j\gamma \in U\lambda^{-1}$. Moreover $u\gamma \in U\gamma \subset U\lambda^{-1}$, and so $u\gamma + (u + v_j)\gamma + v_j\gamma \in U\lambda^{-1}$, whose components are null, except possibly for those of the j-th brick, i.e.

$$u_j\gamma_j + (u_j + v_j)\gamma_j + v_j\gamma_j \in U\lambda^{-1} \cap W_j, \tag{12}$$

which implies that $\operatorname{Im}(\hat{\gamma}_{j_{u_j}}) + u_j\gamma_j \subset U\lambda^{-1} \cap W_j$. Being γ_j 2^δ-differentially uniform, it is also 2^δ-weakly differentially uniform, and since $u_j \neq 0$ we obtain

$$2^{s-\delta-1} < |\operatorname{Im}(\hat{\gamma}_{j_{u_j}})| \leq |U\lambda^{-1} \cap W_j|,$$

therefore $\dim(U\lambda^{-1} \cap W_j) \geq s - d$, which contradicts (11). □

Notice that in the proof of Theorem 4.9 we actually exploited that every S-box is 2^δ-weakly differentially uniform. Hence, we also proved the more general following result.

Theorem 4.10. *Let $\rho = \gamma\lambda \in \operatorname{Sym}(V)$ be the generating function of a wave cipher Φ. If there exists $1 \leq \delta < s$ such that for each $j \in \{1, 2, \ldots, b\}$ the S-box γ_j is*

- *2^δ-weakly differentially uniform,*
- *δ-non-invariant with respect to λ,*

and if $\operatorname{Ker}\lambda = \bigoplus_{j=1}^{b} \operatorname{Ker}\lambda \cap W_j$, then $\langle T_n, \rho \rangle$ is primitive (and so it is $\Gamma_\infty(\Phi)$).

The hypothesis of each S-box being δ-non-invariant w.r.t. λ in Theorem 4.9 can be weakened by adding a reasonable requirement on the diffusion layer. However, for this result does not exist an alternative version using the weak differential uniformity.

Theorem 4.11. *Let $\rho = \gamma\lambda \in \mathrm{Sym}(V)$ be the generating function of a wave cipher Φ. If there exists $1 \leq \delta < s$ such that for each $j \in \{1, 2, \ldots, b\}$ the S-box γ_j is*

- *2^δ-differentially uniform,*
- *$(\delta - 1)$-non-invariant with respect to λ,*

and if the diffusion layer is such that

- $\mathrm{Ker}\,\lambda = \bigoplus_{j=1}^{b} \mathrm{Ker}\,\lambda \cap W_j$,
- $\dim(\mathrm{Ker}\,\lambda \cap W_j) < s - \delta$ *for each* $j \in \{1, 2, \ldots, b\}$,

then $\langle T_n, \rho \rangle$ is primitive (and so it is $\Gamma_\infty(\Phi)$).

Proof. The proof proceeds exactly as that of Theorem 4.9. In this slightly different setting induced from a further requirement on λ, we can conclude that $U \cap V_j \neq \{0\}$. Indeed, being

$$(U \cap V_j)\gamma_j + \mathrm{Ker}\,\lambda \cap W_j = U\lambda^{-1} \cap W_j,$$

and having $\dim(U\lambda^{-1} \cap W_j) \geq s - \delta$ and $\dim(\mathrm{Ker}\,\lambda \cap W_j) < s - \delta$, there must be a non-zero element in $(U \cap V_j)\gamma_j$, and consequently a non-zero element $z \in U \cap V_j$. Then, reasoning as before, using Lemma 4.8 one can prove that $\mathrm{Im}(\hat{\gamma}_{j_z}) \subset U\lambda^{-1} \cap W_j$ and $|\mathrm{Im}(\hat{\gamma}_{j_z})| \geq 2^{s-\delta}$. Moreover, $0 \notin \mathrm{Im}(\hat{\gamma}_{j_z})$, since $z \neq 0$ and γ_j is injective. Hence

$$|U\lambda^{-1} \cap W_j| \geq 2^{s-\delta} + 1,$$

and therefore $\dim(U\lambda^{-1} \cap W_j) \geq s - \delta + 1$. The hypothesis of $(\delta - 1)$-non-invariance of γ_j leads to a contradiction, hence the desired holds. □

5 The security analysis of a concrete instance of wave-cipher

In the previous sections we have introduced a new framework for block ciphers, called wave ciphers, and studied its security with respect to the imprimitivity attack. In particular we primarily aimed at determining sufficient conditions on the choice of the layers which guarantee the resistance of each wave cipher satisfying such conditions against a dangerous algebraic attack. Nevertheless also statistical attacks may represent a threat for the security of these ciphers. However, as already mentioned in Sec. 1, security against statistical attack has to be established considering a specific instance of wave cipher. For this reason, we design a concrete example of a real-world dimension wave cipher by selecting an APN S-box and a proper diffusion layer, and we analyse its resistance against differential and linear

cryptanalysis.

The proposed instance is a 64-bit Feistel Network featuring eight 4×5 APN S-boxes and a 40×32 matrix as diffusion layer. Let us assume $n = 32$, $m = 40$, $s = 4$, $t = 5$ and $b = 8$, and let us consider again the 4×5 S-box γ_1 displayed in Figure 3. Recall that

$$|\{a + b \mid a, b \in \mathrm{Im}(\gamma_1)\}| = 31$$

and $\xi \stackrel{\text{def}}{=} \mathtt{11}_{\mathtt{x}} \notin \{a + b \mid a, b \in \mathrm{Im}(\gamma_1)\}$. Since we want to design a 32-bit invertible generating function for a wave cipher whose confusion layer γ applies 8 copies of the S-box γ_1 and whose diffusion layer features a parallel kernel, we determine a proper diffusion layer λ such that

$$\mathrm{Ker}\,\lambda = \mathrm{Span}_{\mathbb{F}_2}\left\{(\xi,0,0,0,0,0,0,0),(0,\xi,0,0,0,0,0,0),\ldots,(0,0,0,0,0,0,0,\xi)\right\},$$

where 0 denotes the zero vector in $(\mathbb{F}_2)^5$. The matrix displayed in Figure 6 is the chosen example of such a layer. Hence we build the instance of a wave cipher considering $\rho = \gamma\lambda$ as a bijective generating function (see Definition 3.5).

Before analysing statistical attacks, notice that the previously defined layers satisfy the hypotheses of Theorem 4.11 with $\delta = 1$, since γ_1 is 0-non-invariant with respect to $\mathrm{Ker}\,\lambda$, and consequently ρ is such that the group $\langle T_n, \rho\rangle$ is primitive. Then Theorem 4.5 implies that the group $\Gamma_\infty(\Phi)$ generated by the rounds of a wave cipher having $\gamma\lambda$ as generating function is primitive.

In order to discuss resistance against differential and linear cryptanalysis, let us highlight some properties of the chosen diffusion layer, which is inspired by the one of the cipher PRESENT, even though providing slower diffusion. For such cryptanalytic purposes, proceeding as in [10], we can group the eight S-boxes into two groups, as shown in Fig 7. The following properties holds:

1. the input bits to an S-box come from two different S-boxes of the same group;
2. the five output bits for a particular S-box enter two different S-boxes, each of which belongs to a different group in the following round;
3. the output bits of S-boxes of different groups go to different S-boxes;
4. the branch number of λ is $\min_{x \notin \ker(\lambda)} (\mathrm{w}_b(x) + \mathrm{w}_b(x\lambda)) = 2$, where $\mathrm{w}_b(x)$ denotes the number of non-null bricks in the message x.

The study of differential and linear trails, discussed in the following sections, is usually carried out assuming that the key values are random vectors of the same size as the block. For this reason, we decided not to design a concrete instance of key-scheduling algorithm for our cipher.

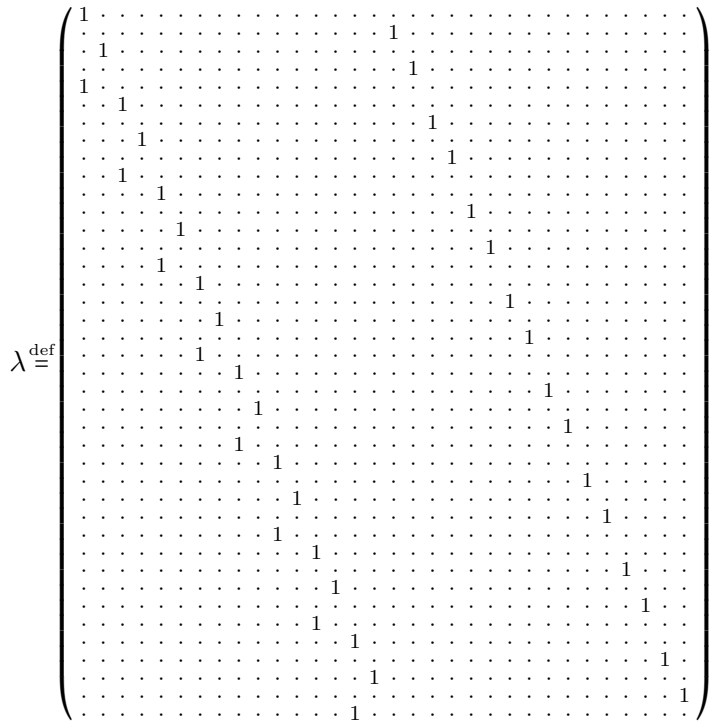

Figure 6: An example of 40×32 proper diffusion layer with parallel kernel, where each "$\cdot$" represents 0.

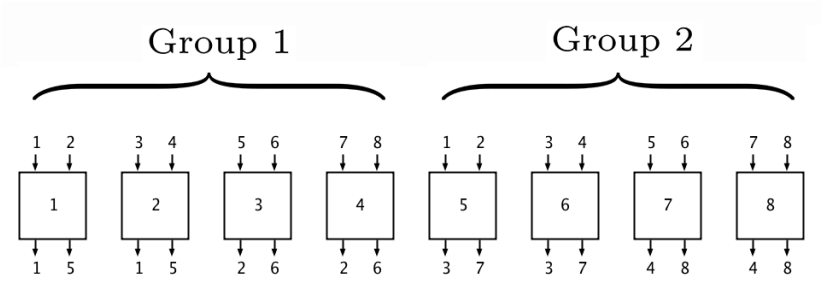

Figure 7: Diffusion properties of the matrix λ of Fig. 6.

5.1 Differential cryptanalysis

The S-box of Fig. 3 is APN, hence all its non-trivial differential probabilities are equal to 2^{-3} and any 3-round differential trail has at least 2 active S-boxes, the worst case being the one forming the pattern 1-0-1, occurring when the XOR with the left part of the difference cancels out the output difference of the F-function for the first round. Consequently, the probability of each 3-round differential trail is upper bounded by

$$\left(2^{-3}\right)^2 = 2^{-6}.$$

Therefore, if $r = 48$, the probability of a single 48-round differential trail is upper bounded by $\left(2^{-6}\right)^{16} = 2^{-96}$.

5.2 Linear cryptanalysis

In the case of linear cryptanalysis, the bias of all linear approximations is less or equal than 2^{-2}. Recalling Matsui's Piling-up Lemma [26], the maximal bias of a linear approximation of three rounds involving two active S-boxes is

$$e_3 = 2 \times \left(2^{-2}\right)^2 = 2^{-3}.$$

Consequently we can bound the maximal bias of a 48-round linear approximation by

$$e_{48} = 2^{15} \times e_3^{16} = 2^{15} \times \left(2^{-3}\right)^{16} = 2^{-33}.$$

Matsui shows in [26] that the number of known plaintexts required in the attack is approximatively e^{-2}, where e denotes the maximal bias of a linear approximation. Therefore an attacker needs approximately 2^{66} known plaintexts to mount a key-recovery linear attack against a 48-round encryption of our instance of wave cipher.

5.3 Other comments

It is worth noting that, although the proposed cipher features S-boxes with an odd number of output bits, the size of the block is a power of two, which represents the optimal case for implementation needs. For example, the disadvantage of considering an FN featuring 5×5 APN S-boxes in place of 4×5 S-boxes would be twofold in terms of keeping the cipher lightweight: from one hand, the size of the block would not be a power of two; from the other hand, a 5×5 APN S-box requires the storage of 32 values, twice the ones needed for a 4×5 S-box.

6 Conclusions and open problems

In this work we proposed a new family of ciphers, called *wave ciphers*, whose round functions are the composition of layers not all invertible. The round functions of a wave cipher are *wave functions*, vectorial Boolean functions obtained as the composition of injective non-linear confusion layers enlarging the message, surjective

linear diffusion layers reducing the message size, and a key addition. Relaxing the requirement that the S-boxes are permutations allowed to consider APN functions to build confusion layers. In particular we gave an example of a 4×5 APN S-box. We proposed to use wave functions as F-functions of Feistel Networks, where computing inverse functions is not required in order to perform decryption. With regard to their security we showed that, under the assumption that the generating function is invertible, and under suitable non-linearity properties of the Boolean functions involved, the group generated by the round functions of a wave ciphers acts primitively. Finally, we presented a concrete example of 64-bit wave cipher and we proved its resistance against differential and linear cryptanalysis, as well as the imprimitivity attack.

Our new construction leaves several problems open, such as determining conditions on the wave functions to ensure that the group generated by the round functions of a wave cipher is the alternating group, or studying the resistance of instances of wave ciphers with respect to other more sophisticated statistical attacks on the wave-shaped structure. Moreover, to the best of our knowledge, $s \times t$ APN functions with $s < t$ are not very much investigated in literature. Finally note that, in order to prove that $\Gamma_\infty(\Phi) = \langle T_{(0,n)}, \overline{\rho} \rangle$ is primitive, we adopted the strategy of considering an SPN having as round functions the same wave functions of Φ, and we used Theorem 4.5 to deduce the primitivity of $\Gamma_\infty(\Phi)$ from the primitivity of $\langle T_n, \rho \rangle$. This forced us to suppose $\rho \in \mathrm{Sym}(V)$. However, the bijectivity of ρ is not required to define a wave cipher. For this reason, one of our interests is to prove the same result in more general hypotheses on ρ.

Acknowledgment The authors are grateful to the anonymous referees for their insightful comments and suggestions, and to Andrea Visconti for several useful discussions. This work has been partially presented at the 13th International Conference on Finite Fields and their Applications (Fq13). Some of the results showed in this paper are included in R. Civino's PhD thesis (supervised by M. Sala) and in I. Zappatore's Master thesis (supervised by R. Aragona, M. Calderini, and M. Sala).

R. Aragona is member of INdAM-GNSAGA (Italy). R. Civino thankfully acknowledges support by the Department of Mathematics of the University of Trento. R. Aragona, R.Civino, and M. Sala thankfully acknowledge support by MIUR-Italy via PRIN 2015TW9LSR "Group theory and applications".

References

[1] C. Adams, *The CAST-128 encryption algorithm*, (1997); available at `http://buildbot.tools.ietf.org/html/rfc2144`.

[2] R. J. Anderson, E. Biham, and L. R. Knudsen, *SERPENT: A new block cipher proposal*, Fast Software Encryption, 222–238, Lecture Notes in Comput. Sci. **1372**, Springer, Berlin (1998).

[3] K. Aoki, et al. *Camellia: A 128-bit block cipher suitable for multiple platforms-design and analysis*, Selected Areas in Cryptography. 39–56, Lecture Notes in Comput. Sci., **2012**, Springer, Berlin (2000).

[4] R. Aragona, M. Calderini, A. Tortora, and M. Tota, *On the primitivity of PRESENT and other lightweight ciphers*, J. Algebra Appl. **17** (2017), no. 6, 1850115 (16 pages).

[5] R. Aragona, A. Caranti, F. Dalla Volta, and M. Sala, *On the group generated by the round functions of translation based ciphers over arbitrary fields*, Finite Fields Appl. **25** (2014), 293–305.

[6] R. Aragona, A. Caranti, and M. Sala, *The group generated by the round functions of a GOST-like cipher*, Ann. Mat. Pura Appl., **196** (2016), no. 1, 1–17.

[7] A. Bannier, N. Bodin, and E. Filiol, *Partition-Based Trapdoor Ciphers*, IACR Cryptology ePrint Archive, Report 2016/493 (2016); available at `http://eprint.iacr.org/2016/493`.

[8] E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, J. Cryptology **4** (1991), no. 1, 3–72.

[9] K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe, *An APN permutation in dimension six*. Finite Fields: theory and applications, **518** (2010), 33–42.

[10] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin and C. Vikkelsoe, *PRESENT: An ultra-lightweight block cipher*, CHES '07, 450–466, Lecture Notes in Comput. Sci. **4727**, Springer, Berlin (2007).

[11] M. Calderini, *A note on some algebraic trapdoors for block ciphers*, to appear in Advances in Mathematics of Communications, (2018); available at `https://arxiv.org/abs/1705.08151`.

[12] M. Calderini, and M. Sala *Elementary abelian regular subgroups as hidden sums for cryptographic trapdoors*, preprint, arXiv:1702.00581 [math.GR] (2017).

[13] M. Calderini, I. Villa, and M. Sala, *A note on APN permutations in even dimension*, Finite Fields Appl. **46**, (2017), 1–16.

[14] P. J. Cameron, *Permutation groups*, London Mathematical Society Student Texts **45**, Cambridge University Press, Cambridge (1999).

[15] A. Canteaut, S. Duval, and L. Perrin, *A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size* 2^{4k+2}, IEEE Transactions on Information Theory (2017).

[16] A. Canteaut and M. Naya-Plasencia, *Structural weaknesses of permutations with low differential uniformity and generalized crooked functions*, Finite Fields: Theory and Applications-Selected Papers from the 9th International Conference Finite Fields and Applications, Contemporary Mathematics, **518** (2010), 55-71.

[17] A. Caranti, F. Dalla Volta, and M. Sala, *An application of the O'Nan-Scott theorem to the group generated by the round functions of an AES-like cipher*, Des. Codes Cryptogr. **52** (2009), no. 3, 293–301.

[18] A. Caranti, F. Dalla Volta, and M. Sala, *On some block ciphers and imprimitive groups*, Appl. Algebra Engrg. Comm. Comput. **20** (2009), no. 5-6, 339–350.

[19] D. Coppersmith and E. Grossman, *Generators for certain alternating groups with applications to cryptography*, SIAM J. Appl. Math. **29** (1975), no. 4, 624–627.

[20] J. Daemen and V. Rijmen, *The design of Rijndael: AES – the Advanced Encryption Standard*, Information Security and Cryptography, Springer-Verlag, Berlin (2002).

[21] V. Dolmatov, *GOST 2814789: encryption, decryption, and message authentication code (MAC) algorithms*, Technical report (2010); available at `http://tools.ietf.org/html/rfc5830`.

[22] Federal information processing standards publication, *Data Encryption Standard and others*, National Bureau of Standards, US Department of Commerce (1977).

[23] E. Goursat, *Sur les substitutions orthogonales et les divisions régulières de l'espace*, Ann. Sci. École Norm. Sup. 3(6) (1889), 9–102.

[24] X.-D. Hou. *Affinity of permutations of* $\mathbb{F}_2^n$. Discrete Appl. Math., **154** (2006), no. 2, 313–325.

[25] Jr. B. S. Kaliski, R. L. Rivest, and A. T. Sherman, *Is the Data Encryption Standard a group? (Results of cycling experiments on DES)*, J. Cryptology **1** (1988), no. 1, 3–36.

[26] M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Advances in cryptology – EUROCRYPT '93, 386–397, Lecture Notes in Comput. Sci. **765**, Springer, Berlin (1994).

[27] K. Nyberg, *Differentially uniform mappings for cryptography*, Advances in cryptology – EUROCRYPT '93, 55–64, Lecture Notes in Comput. Sci. **765**, Springer, Berlin (1994).

[28] K. G. Paterson, *Imprimitive permutation groups and trapdoors in iterated block ciphers*, Fast Software Encryption, 201–214, Lecture Notes in Comput. Sci. **1636**, Springer, Berlin (1999).

[29] J. Petrillo, *Goursat's other theorem*, The College Mathematics Journal 40(2) (2009), 119–124.

[30] G. Piret, T. Roche, and C. Carlet, *PICARO–a block cipher allowing efficient higher-order side-channel resistance*, Applied Cryptography and Network Security–ACNS2012, Lecture Notes in Comput. Sci. **7341**, Springer, Berlin (2012).

[31] R. Sparr and R. Wernsdorf, *Group theoretic properties of Rijndael-like ciphers*, Discrete Appl. Math. **156** (2008), no. 16, 3139–3149.

[32] C. E. Shannon, *Communication theory of secrecy systems*, Bell System Tech. **28** (1949), 656–715.

[33] R. Wernsdorf, *The round functions of RIJNDAEL generate the alternating group*, Fast Software Encryption 143-148, Lecture Notes in Comput. Sci. **2365**, Springer, Berlin (2002).

[34] R. Wernsdorf, *The one-round functions of the DES generate the alternating group*, Advances in Cryptology-EUROCRYPT '92, Lecture Notes in Comput. Sci. **658**, Springer, Berlin (1993).

[35] R. Wernsdorf, *The round functions of SERPENT generate the alternating group*, (2000); available at `http://csrc.nist.gov/archive/aes/round2/\comments/20000512-rwernsdorf.pdf`.

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x	10_x	11_x	12_x	13_x	14_x	15_x	16_x	17_x	18_x	19_x	$1A_x$	$1B_x$	$1C_x$	$1D_x$	$1E_x$	$1F_x$
16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
0_x	·	·	·	·	·	·	·	·	·	2	2	2	·	·	·	·	·	·	·	2	·	·	2	·	·	2	2	·	·	·	·	2
1_x	·	·	·	2	·	2	·	·	·	·	2	·	2	·	·	2	·	·	·	2	·	·	2	·	·	·	·	2	·	·	·	·
2_x	·	·	·	·	·	2	·	·	2	·	·	·	2	·	·	·	2	·	·	·	·	2	·	·	·	2	·	·	·	·	·	2
3_x	·	·	·	·	·	·	·	·	·	2	·	·	2	·	·	·	·	·	·	2	·	·	2	·	·	·	·	·	·	2	2	·
4_x	·	·	·	·	·	·	·	·	·	·	·	·	2	·	·	2	·	·	·	·	·	2	2	·	·	2	·	·	2	·	·	·
5_x	·	·	·	·	·	·	2	·	·	·	·	·	2	·	·	2	2	·	·	·	·	·	2	2	·	·	2	·	·	·	·	2
6_x	·	·	·	2	·	·	2	·	·	·	·	·	·	·	·	2	·	·	2	2	·	·	·	·	·	2	·	·	2	·	·	2
7_x	·	·	·	2	2	·	2	·	·	·	2	·	2	·	·	·	·	·	·	·	·	2	·	·	·	2	2	·	·	·	·	·
8_x	·	·	·	2	·	2	·	·	·	·	·	·	·	2	·	·	·	·	·	·	·	2	2	·	·	·	2	·	2	·	·	2
9_x	·	·	·	·	·	2	2	·	·	2	2	·	·	·	·	2	·	·	·	·	2	2	·	·	·	·	·	·	·	·	·	2
A_x	·	2	·	·	·	·	2	·	·	·	2	·	·	·	·	·	2	·	·	2	·	2	2	·	·	·	·	·	2	·	·	·
B_x	·	·	·	·	·	2	·	·	·	·	2	·	·	·	·	2	2	·	·	·	·	·	·	·	·	2	2	·	2	·	2	·
C_x	·	·	·	2	·	·	·	·	·	2	·	·	·	·	·	2	2	·	·	2	·	2	·	·	2	·	2	·	·	·	·	·
D_x	·	·	2	·	·	2	2	·	·	2	·	·	2	·	·	·	·	·	·	2	·	·	·	·	·	·	2	·	2	·	·	·
E_x	·	·	·	2	·	·	·	·	·	2	2	·	2	·	2	·	2	·	·	·	·	·	·	·	·	·	2	·	2	·	·	2
F_x	·	·	·	2	·	2	2	2	·	·	2	·	2	·	·	·	2	·	·	·	·	2	2	·	·	2	·	·	·	·	·	·